

PR4



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,375	06/30/2000	Curtis E. Ide	05456.105004	8222

7590 03/25/2004
King & Spalding
45th Floor
191 Peachtree Street N E
Atlanta, GA 30303

EXAMINER

JACKSON, JENISE E

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 03/25/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/607,375

Applicant(s)

IDE ET AL.

Examiner

Jenise E Jackson

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date Z.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dinh et al. in view of Hummel, Jr. et al.

3. As per claim 1, Dinh et al. discloses authenticating a workstation requesting a network service from a network server via a computer network, generating workstation security credentials, by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network(see col. 7, lines 1-35); comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the service(see col. 7, lines 27-64, col. 8, lines 24-33); and authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy(see col. 7, lines 27-64, col. 8, lines 24-33). Dinh does not disclose denying access to the network service by the workstation. However, Hummel, Jr. et al. discloses providing a log-in page and providing an error message when denying access to the network service(see col. 9, line 44 through col. 10, lines 12). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Dinh et al. to provide an error page as taught by Hummel, Jr.

Art Unit: 2131

et al. to provide delivery of protected software wherein business rules are utilized to authenticate and authorize access to users(see abstract).

5. As per claim 2, Dinh discloses the step of authorizing access to a predetermined level of the network service if the workstation security credentials satisfy a portion of the workstation security policy(see col. 7, lines 27-44).

6. As per claim 3, Dinh et al. discloses wherein the step of generating the workstation security credentials includes completing the vulnerability assessment of the workstation by a local workstation assessment service maintained on the workstation, the local workstation assessment service operative to generate the workstation security credentials(see col. 7, lines 14-67).

7. As per claim 4, Dinh et al. discloses wherein the workstation security policy is maintained on the workstation, the process further includes the step of providing the workstation security credentials from the local workstation assessment service to the workstation security policy(see col. 7, lines 27-64, col. 8, lines 24-33).

8. As per claim 5, Dinh et al. discloses wherein the step of generating the workstation security credentials includes completing the vulnerability assessment of the workstation by a network workstation assessment service maintained on the network server, the network workstation assessment service operative to generate the workstation security credentials(see col. 7, lines 27-64, col. 8, lines 24-33).

9. As per claim 6, Dinh et al. discloses wherein the workstation security policy is maintained on the workstation, the process further includes the step of providing the workstation

Art Unit: 2131

security credentials from the network workstation assessment service to the workstation security policy on the workstation via the computer network(see col. 7, lines 30-47).

10. As per claim 7, limitations have already been addressed see claim 1. Further, as per claim 7, the assessment server operating as a remote server different from the network server, the network workstation assessment service operative to generate the workstation security credentials(see col. 7, lines 27-64, col. 8, lines 24-33).

11. As per claim 8, limitations have already been addressed(see claim 1).

12. As per claim 9, Dinh et al. discloses the step of communicating a service decision from the network server to the workstation via the computer network, the service decision defining whether the workstation is allowed to access the network service(see col. 7, lines 27-64).

13. As per claim 10, Dinh et al. discloses wherein the step of generating the workstation security credentials includes completing the vulnerability assessment of the workstation by the network service on the network server in response to receiving a request for the network service from the workstation via the computer network(see col. 7, lines 1-35).

14. As per claim 11, Dinh et al. discloses wherein the workstation security policy is maintained on the network server, the process further including the step of comparing at the network server the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service(see col. 7, lines 27-64, col. 8, lines 24-33).

15. As per claim 12, it is rejected under the same basis as claim 1.

16. As per claim 13, limitations have already been addressed(see claim 1).

Art Unit: 2131

17. As per claim 14, Dinh et al. discloses including a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network(see col. 7, lines 27-64, col. 8, lines 24-33).

18. As per claim 15, Dinh et al. discloses wherein the network service is further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service (see col. 7, lines 27-64, col. 8, lines 24-33), the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy(see col. 8, lines 24-33).

19. As per claim 16, limitations have already been addressed(see claim 1).

20. As per claim 17, Dinh et al. discloses including a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network(see col. 7, lines 27-44).

21. As per claim 18, Dinh et al. discloses wherein the network service is further operative to compare the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy(see col. 7, lines 27-64, col. 8, lines 24-33).

22. As per claim 19, Dinh et al. discloses issuing a request for a log-in page to a network server from a browser operating on the workstation; transmitting the log-in page and an

Art Unit: 2131

authentication plug-in from the network server to the workstation via the compute network, the authentication plug-in installable within the browser(see col. 7, lines 35-44) and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network(see col. 7, lines 27-64); transmitting the workstation security credentials from the authentication plug-in to the network server via the computer network; and determining at a CGI script operating on the network server whether the workstation should be granted access to a software service of the network based on the workstation security credentials(see col. 7, lines 27-64, col. 8, lines 24-33).

23. As per claim 20, limitations have already been addressed(see claim 1). Further, claim 20, Dinh et al. is rejected of the CGI script(see col. 6, lines 33-55, col. 7, lines 27-44).

21. As per claim 21, Dinh et al. discloses a network assessment service operating on a network workstation assessment server on the computer network, the network assessment service operative to generate workstation security credentials by completing a vulnerability assessment of the workstation via the computer network to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network(see col. 7, lines 27-64, col. 8, lines 24-33), the network service, responsive to receiving the workstation security credentials from the network assessment service via the computer, operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials and the user credentials(see col. 7, lines 27-64, col. 8, lines 24-33).

Art Unit: 2131

22. As per claim 22, Dinh et al. discloses including a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network(see col. 6, lines 33-55).

23. As per claim 23, Dinh et al. discloses wherein the network service is further operative to compare the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service (col. 7, lines 27-64, col. 8, lines 24-33), the network service operative to authorize access to the software service by the workstation if the workstation security credentials and the user credentials satisfy the workstation security policy(see col. 7, lines 27-44).

24. As per claim 24, Dinh et al. discloses wherein the network service is operative to transmit to the network assessment service via the computer network a request to complete the vulnerability assessment of the workstation in response to receiving a request for the software service from the workstation(see col. 7, lines 27-64, col. 8, lines 24-33).

25. As per claim 25, Dinh et al. discloses issuing a request for a log-in page to a network server from a browser operating on the workstation; transmitting the log-in page, an authentication plug-in(see col. 7, lines 35-44), and a workstation policy from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network(see col. 7, lines 27-64); comparing the workstation security credentials to the workstation policy on the workstation to determine

Art Unit: 2131

whether the workstation should be granted access to a software service of the network(col. 7, lines 27-64, col. 8, lines 24-33).

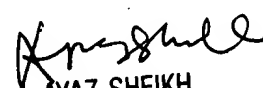
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).




AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100